

DEPARTMENT OF DEFENSE
DIRECTIVES SYSTEM TRANSMITTAL

NUMBER

5220.22-M, Change 1

July 31, 1997

Special

ATTACHMENTS

32 Pages

INSTRUCTIONS FOR RECIPIENTS

The following page changes to DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1995, are authorized:

PAGE CHANGES

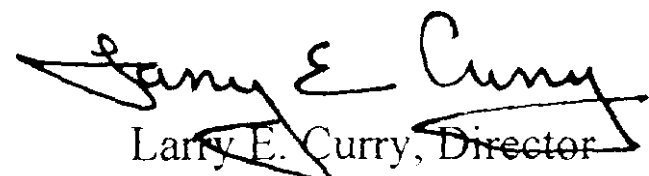
Remove: Pages 1-1-1 through 1-1-3, 2-2-1 through 2-2-5, 3-1-1, 4-1-1 through 4-2-6, 5-2-1, 9-1-1 through 9-1-3, 10-3-1 and 10-3-2, 11-3-1, C-1 through C-8

Insert: Attached replacement pages

Changes appear on pages 1-1-1 through 1-1-3, 2-2-1, 2-2-4, 3-1-1, 4-1-1 through 4-1-3, 4-2-2 through 4-2-4, 4-2-6, 5-2-1, 9-1-1, 9-1-2, 10-3-1, 11-3-1, C-2, C-6 through C-8 and are indicated by marginal change bars.

EFFECTIVE DATE

The above changes are effective immediately.


Larry E. Curry, Director
Correspondence and Directives

WHEN PRESCRIBED ACTION HAS BEEN TAKEN, THIS TRANSMITTAL SHOULD BE FILED WITH THE BASIC DOCUMENT

Chapter 1.

General Provisions and Requirements

Section 1. Introduction

1-100. Purpose. This Manual is issued in accordance with the National Industrial Security Program (NISP). The Manual prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. The Manual also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.

1-101. Authority.

a. The NISP was established by Executive Order 12829, 6 January 1993, "National Industrial Security Program" for the protection of information classified pursuant to Executive Order 12958, April 17, 1995, "Classified National Security Information," or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated Executive Agent for the NISP by the President. The Director, Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

b. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission and the Director of Central Intelligence is responsible for issuance and maintenance of this Manual. The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended. The Director of Central Intelligence shall prescribe that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information. The

Director of Central Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of Central Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information. The Secretary of Energy and the Nuclear Regulatory Commission retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954, as amended. The Secretary or the Commission may inspect and monitor contractor, licensee, grantee, and certificate holder programs and facilities that involve access to such information.

c. The Secretary of Defense serves as Executive Agent for inspecting and monitoring contractors, licensees, grantees, and certificate holders who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, certificate holders, and grantees and their respective employees. The Heads of agencies shall enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on their behalf.

d. The Director, ISOO, will consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the NISP.

e. Nothing in this Manual shall be construed to supersede the authority of the Secretary of Energy or the Chairman of the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; or detract from the authority of installation Commanders under the Internal Security Act of 1950; the authority of the Director of Central Intelligence under the National Security Act of 1947, as amended, or Executive Order No. 12333 of December 8, 1981; or the authority of any other federal department or agency Head granted pursuant to U.S. statute or Presidential decree.

1-102. Scope.

a. The NISP applies to all executive branch departments and agencies and to all cleared contractor facilities located within the United States, its Trust Territories and Possessions.

b. This Manual applies to and shall be used by contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination. This Manual also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to contractors that requires protection in the interest of national security. The Manual implements applicable Federal Statutes, Executive orders, National Directives, international treaties, and certain government-to- government agreements.

c. If a contractor determines that implementation of any provision of this Manual is more costly than provisions imposed under previous U.S. Government policies, standards or requirements, the contractor shall notify the Cognizant Security Agency (CSA). The notification shall indicate the prior policy, standard or requirement and explain how the NISPOM requirement is more costly to implement. Contractors shall, however, implement any such provision within three years from the date of this Manual, unless a written exception is granted by the CSA. When implementation is determined to be cost neutral, or where cost savings or cost avoidance can be achieved, implementation by contractors shall be effected no later than 6 months from the date of this Manual.

d. This Manual does not contain protection requirements for Special Nuclear Material.

1-103. Agency Agreements.

a. E.O. 12829 requires the heads of agencies to enter into agreements with the Secretary of Defense that establish the terms of the Secretary's responsibilities on behalf of these agency heads.

b. The Secretary of Defense has entered into agreements with the departments and agencies listed below for the purpose of rendering industrial security services. This delegation of authority is contained in an exchange of letters between the Secretary of Defense and: (1) The Administrator, National Aeronautics and Space Administration (NASA); (2) The Secretary of Commerce; (3) The Administrator, General Services Administration (GSA); (4) The Secretary of State; (5) The Administrator, Small Business Administration (SBA); (6) The Director, National Science Foundation [NSF]; (7) The Secretary of the Treasury; (8) The Secretary of Transportation; (9) The Secretary of the Interior; (10)

The Secretary of Agriculture; (11) The Director, United States Information Agency (USIA); (12) The Secretary of Labor; (13) The Administrator, Environmental Protection Agency (EPA); (14) The Attorney General, Department of Justice; (15) The Director, U.S. Arms Control and Disarmament Agency (ACDA); (16) The Director, Federal Emergency Management Agency (FEMA); (17) The Chairman, Board of Governors, Federal Reserve System (FRS); (18) The Comptroller General of the United States, General Accounting Office (GAO); (19) The Director of Administrative Services, United States Trade Representative (USTR); and (20) The Director of Administration, United States International Trade Commission (USITC); (21) The Administrator, United States Agency for International Development and (22) The Executive Director for Operations of the Nuclear Regulatory Commission. NOTE: Interagency agreements have not been effected with the Department of Defense by the Department of Energy and the Central Intelligence Agency.

1-104. Security Cognizance.

a. Consistent with 1-101 e, above, security cognizance remains with each federal department or agency unless lawfully delegated. The term "Cognizant Security Agency" (CSA) denotes the Department of Defense (DoD), the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency. The Secretary of Defense, the Secretary of Energy, the Director of Central Intelligence and the Chairman, Nuclear Regulatory Commission may delegate any aspect of security administration regarding classified activities and contracts under their purview within the CSA or to another CSA. Responsibility for security administration may be further delegated by a CSA to one or more "Cognizant Security Offices (CSO)." It is the obligation of each CSA to inform industry of the applicable CSO.

b. The designation of a CSO does not relieve any Government Contracting Activity (GCA) of the responsibility to protect and safeguard the classified information necessary for its classified contracts, or from visiting the contractor to review the security aspects of such contracts.

c. Nothing in this Manual affects the authority of the Head of an Agency to limit, deny, or revoke access to classified information under its statutory, regulatory, or contract jurisdiction if that Agency Head determines that the security of the

nation so requires. The term “agency head” has the meaning provided in 5 U.S.C. 552(f).

1-105. Composition of Manual. This Manual is comprised of a “baseline” portion (Chapters 1 through 11). That portion of the Manual that prescribes requirements, restrictions, and safeguards that exceed the baseline standards, such as those necessary to protect special classes of information, are included in the **NISPOM Supplement (NISPOMSUP)**. Until officially revised or canceled, the existing **COMSEC** and Carrier Supplements to the former “Industrial Security Manual for Safeguarding Classified Information” will continue to be applicable to DoD-cleared facilities only.

1-106. Manual Interpretations. All contractor requests for interpretations of this Manual shall be forwarded to the Cognizant Security Agency (CSA)

through its designated Cognizant Security Office (CSO). Requests for interpretation by contractors located on any U.S. Government installation shall be forwarded to the **CSA** through the Commander or Head of the host installation. Requests for interpretation of **DCIDs** referenced in the **NISPOM Supplement** shall be forwarded to the **DCI** through approved channels.

1-107. Waivers and Exceptions to this Manual. Requests shall be submitted by industry through government channels approved by the CSA. When submitting a request for waiver, the contractor shall specify, in writing, the reasons why it is impractical or unreasonable to comply with the requirement. Waivers and exceptions will not be granted to impose more stringent protection requirements than this Manual provides for **CONFIDENTIAL**, **SECRET**, or **TOP SECRET** information.

Section 2. Personnel Clearances

2-200. General.

a. An employee may be processed for a personnel clearance (PCL) when the contractor determines that access is essential in the performance of tasks or services related to the fulfillment of a classified contract. A PCL is valid for access to classified information at the same, or lower, level of classification as the level of the clearance granted.

b. The CSA will provide written notice when an employee's PCL has been granted, denied, suspended, or revoked. The contractor shall immediately deny access to classified information to any employee when notified of a denial, revocation or suspension. The CSA will also provide written notice when processing action for PCL eligibility has been discontinued. Contractor personnel may be subject to a reinvestigation program as specified by the CSA.

c. Within a multiple facility organization (MFO), PCLS will be issued to a company's home office facility (HOF) unless an alternative arrangement is approved by the CSA. Cleared employee transfers within an MFO, and classified access afforded thereto, shall be managed by the contractor.

d. The contractor shall limit requests for PCLS to the minimal number of employees necessary for operational efficiency, consistent with contractual obligations and other requirements of this Manual. Requests for PCLS shall not be made to establish "pools" of cleared employees.

e. The contractor shall not submit a request for a PCL to one agency if the employee applicant is cleared or is in process for a PCL by another agency. In such cases, to permit clearance verification, the contractor should provide the new agency with the full name, date and place of birth, current address, social security number, clearing agency, and type of clearance.

2-201. Investigative Requirements. Investigations conducted by a Federal Agency shall not be duplicated by another Federal Agency when those investigations are current within 5 years and meet the scope and standards for the level of PCL required. The types of investigations required are as follows:

a. Single Scope Background Investigation (SSBI). An SSBI is required for TOP SECRET, Q, and SCI access. Investigative requests shall be made using the SF 86.

b. National Agency Check with Local Agency Check and Credit Check (NACLIC). An NACLIC is required for a SECRET, L, and CONFIDENTIAL PCL. Investigative requests shall be made using the SF 86.

c. Polygraph. Agencies with policies sanctioning the use of the polygraph for PCL purposes may require polygraph examinations when necessary. If issues of concern surface during any phase of security processing, coverage will be expanded to resolve those issues.

2-202. Common Adjudicative Standards. Security clearance and SCI access determinations shall be based upon uniform common adjudicative standards.

2-203. Reciprocity. Federal agencies that grant security clearances (TOP SECRET, SECRET, CONFIDENTIAL, Q or L) to their employees or their contractor employees are responsible for determining whether such employees have been previously cleared or investigated by the Federal Government. Any previously granted PCL that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance required, shall provide the basis for issuance of a new clearance without further investigation or adjudication unless significant derogatory information that was not previously adjudicated becomes known to the granting agency.

2-204. **Pre-employment** Clearance Action. Contractors shall not initiate any pre-employment clearance action unless the recruitment is for a specific position that will require access to classified information. Contractors shall include the following statement in such employment advertisements: "Applicants selected will be subject to a government security investigation and must meet eligibility requirements for access to classified information." The completed PCL application may be submitted to the CSA by the contractor prior to the date of employment, provided a written commitment for employment has been made by the contractor that prescribes a fixed date for employment within the ensuing 180 days, and the candidate has accepted the employment offer in writing.

2-205. Contractor-Granted Clearances. Contractors are no longer permitted to grant clearances. Contractor-granted Confidential clearances in effect under previous policy are not valid for access to: Restricted Data; Formerly Restricted Data; COMSEC information; Sensitive

Compartmented Information; NATO information (except RESTRICTED); Critical or Controlled Nuclear Weapon Security positions; and classified foreign government information.

2-206. Verification of U.S. Citizenship. The contractor shall require each applicant for a PCL who claims U.S. citizenship to produce evidence of citizenship. A PCL will not be granted until the contractor has certified the applicant's U.S. citizenship.

2-207. Acceptable Proof of Citizenship.

a. For individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar's signature. It must bear the raised, impressed, or multicolored seal of the registrar's office. The only exception is if a state or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable. A delayed birth certificate is one created when a record was filed more than one year after the date of birth. Such a certificate is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include: baptismal or circumcision certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of birth. Other documentary evidence can be early census, school, or family bible records, newspaper files, or insurance papers. All documents submitted as evidence of birth in the U.S. shall be original or certified documents.

b. If the individual claims citizenship by naturalization, a certificate of naturalization is acceptable proof of citizenship.

c. If citizenship was acquired by birth abroad to a U.S. citizen parent or parents, the following are acceptable evidence:

(1) A Certificate of Citizenship issued by the Immigration and Naturalization Service (INS); or

(2) A Report of Birth Abroad of a Citizen of the United States of America (Form FS-240); or

(3) A Certificate of Birth (Form FS-545 or DS-1350).

d. A passport, current or expired, is acceptable proof of citizenship.

e. A Record of Military Processing-Armed Forces of the United States (DD Form 1966) is acceptable proof of citizenship, provided it reflects U.S. citizenship.

2-208. Letter of Notification of Personnel Clearance (**LOC**). An LOC will be issued by the CSA to notify the contractor that its employee has been granted a PCL. Unless terminated, suspended or revoked by the Government, the LOC remains effective as long as the employee is continuously employed by the contractor.

2-209. Representative of a Foreign Interest. The CSA will determine whether a Representative of a Foreign Interest (**RFI**) is eligible for a clearance or continuation of a clearance.

a. An RFI must be a U.S. citizen to be eligible for a PCL.

b. The RFI shall submit a statement that fully explains the foreign connections and identifies all foreign interests. The statement shall contain the contractor's name and address and the date of submission. If the foreign interest is a business enterprise, the statement shall explain the nature of the business and, to the extent possible, details as to its ownership, including the citizenship of the principal owners or blocks of owners. The statement shall fully explain the nature of the relationship between the applicant and the foreign interest and indicate the approximate percentage of time devoted to the business of the foreign interest.

2-210. Non-U. S. Citizens. Only U.S. citizens are eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national. Such individuals may be granted a Limited Access Authorization (LAA) in those rare circumstances where the non-U. S. citizen possesses unique or unusual skill or expertise that is urgently needed to support a specific U.S. Government contract involving access to specified classified information and a cleared or clearable U.S. citizen is not readily available. In addition, the LAA may only be issued under the following circumstances:

a. With the concurrence of the GCA in instances of special expertise.

b. With the concurrence of the CSA in furtherance of U.S. Government obligations pursuant to U.S. law, treaty, or international agreements.

2-211. Access Limitations of an LAA. An LAA granted under the provisions of this Manual is not valid for access to the following types of information.

a. TOP SECRET information;

b. Restricted Data or Formerly Restricted Data;

c. Information that has not been determined releasable by a U.S. Government Designated Disclosure Authority to the country of which the individual is a citizen;

d. COMSEC information;

e. Intelligence information;

f. NATO Information. However, foreign nationals of a NATO member nation may be authorized access to NATO Information provided that: (1) A NATO Security Clearance Certificate is obtained by the CSA from the individual's home country; and (2) NATO access is limited to performance on a specific NATO contract.

g. Information for which foreign disclosure has been prohibited in whole or in part; and

h. Information provided to the U.S. Government in confidence by a third party government and classified information furnished by a third party government.

2-212. Interim Clearances. Interim TOP SECRET PCLS shall be granted only in emergency situations to avoid crucial delays in precontract negotiation, or in the award or performance on a contract. The contractor shall submit applications for Interim TOP SECRET PCLS to the pertinent GCA for endorsement. Applicants for TOP SECRET, SECRET, and CONFIDENTIAL PCLS may be routinely granted interim PCLS at the SECRET or CONFIDENTIAL level, as appropriate, provided there is no evidence of adverse information of material significance. The interim status will cease if results are favorable following completion of full investigative requirements. .4[that time the CSA will

issue a new LOC. Non-U.S. citizens are not eligible for interim clearances.

a. An interim SECRET or CONFIDENTIAL PCL is valid for access to classified information at the level of the interim PCL granted, except for Sensitive Compartmented Information, Restricted Data, COMSEC Information, SAP, and NATO information. An interim TOP SECRET PCL is valid for access to TOP SECRET information and Restricted Data, NATO Information and COMSEC information at the SECRET and CONFIDENTIAL level.

b. An interim PCL granted by the CSA negates any existing contractor-granted CONFIDENTIAL clearance. When an interim PCL has been granted and derogatory information is subsequently developed, the CSA may withdraw the interim pending completion of the processing that is a prerequisite to the granting of a final PCL.

c. When an interim PCL for an individual who is required to be cleared in connection with the FCL is withdrawn, the interim FCL will also be withdrawn, unless action is taken to remove the individual from the position requiring access.

d. Withdrawal of an interim PCL is not a denial or revocation of the clearance and is not appealable during this stage of the processing.

2-213. Consultants. A consultant is an individual under contract to provide professional or technical assistance to a contractor or GCA in a capacity requiring access to classified information. The consultant shall not possess classified material off the premises of the using (hiring) contractor or GCA except in connection with authorized visits. The consultant and the using contractor or GCA shall jointly execute a consultant certificate setting forth respective security responsibilities. The using contractor or GCA shall be the consumer of the services offered by the consultant it sponsors for a PCL. For security administration purposes, the consultant shall be considered an employee of the hiring contractor or GCA. The CSA shall be contacted regarding security procedures to be followed should it become necessary for a consultant to have custody of classified information at the consultant's place of business.

2-214. Concurrent PCLS. A concurrent PCL can be issued if a contractor hires an individual or engages a consultant who has a current PCL (LOC issued to another contractor). The gaining contractor must be

issued an LOC prior to the employee having access to classified information at that facility. Application **shall** be made by the submission of the CSA designated form.

2-215. Converting PCLS to Industrial Clearances. PCLS granted by government agencies may be converted to industrial clearances when: (a) A determination can be made that the investigation meets standards prescribed for such clearances; (b) No more than 24 months has lapsed since the date of termination of the clearance; and, (c) No evidence of adverse information exists since the last investigation. Contractors employing persons eligible for conversion of clearance may request clearance to the level of access required by submitting the CSA designated form to the CSA. Access may not be granted until receipt of the LOC. The following procedures apply.

a. Former DOE and NRC Personnel. A Q access authorization can be converted to a TOP SECRET clearance. An L access authorization can be converted to a SECRET clearance. Annotate the application: "DOE (or NRC) Q (or L) Conversion Requested."

b. Federal Personnel. Submit a copy of the "Notification of Personnel Action" (Standard Form 50), which terminated employment with the Federal Government with the application.

c. Military Personnel. Submit a copy of the "Certificate of Release or Discharge From Active Duty" (DD Form 214).

d. National Guard and Reserve Personnel in the Ready Reserve Program. Include the individual's service number, the identity and exact address of the unit to which assigned, and the date such participation commenced on the application. For those individuals who have transferred to the standby or retired Reserve, submit a copy of the order effecting such a transfer.

2-216. Clearance Terminations. The contractor shall terminate a PCL (a) Upon termination of employment; or (b) When the need for access to

classified information in the future is reasonably foreclosed. Termination of a PCL is accomplished by submitting a **CSA-designated** form to the CSA.

2-217. Clearance Reinstatements. A PCL can be reinstated provided (a) No more than 24 months has lapsed since the date of termination of the clearance; (b) There is no known adverse information; (c) The most recent investigation must not exceed 5 years (TS, Q) or 10 years (SECRET, L); and (d) Must meet or exceed the scope of the investigation required for the level of PCL that is to be reinstated or granted. A PCL can be reinstated at the same, or lower, level by submission of a CSA-designated form to the CSA. The employee may not have access to classified information until receipt of the LOC.

2-218. Procedures for Completing the SF 86. The SF 86 shall be completed jointly by the employee and the contractor. Contractors shall inform employees that part 2 of the SF 86 may be completed in private and returned to security personnel in a sealed envelope. The contractor shall not review any information that is contained in the sealed envelope. The contractor shall review the remainder of the application to determine its adequacy and to ensure that necessary information has not been omitted. The contractor shall ensure that the applicant's fingerprints are authentic, legible, and complete to avoid subsequent clearance processing delays. An employee of the contractor shall witness the taking of the applicant's fingerprints to ensure that the person fingerprinted is, in fact, the same as the person being processed for the clearance. All PCL forms required by this Section are available from the CSA.

2-219. Records Maintenance. The contractor shall maintain a current record at each facility (to include uncleared locations) of all cleared employees. Records maintained by a HOF and/or PMF for employees located at subordinate facilities (cleared and uncleared locations) shall include the name and address at which the employee is assigned. When furnished with a list of cleared personnel by the CSA, contractors are requested to annotate the list with any corrections or adjustments and return it at the earliest practical time. The reply shall include a statement by the FSO certifying that the individuals listed remain employed and that a PCL is still required.

Chapter 3.

Security Training and Briefings

Section 1. Security Training and Briefings

3-100. General. Contractors shall provide all cleared employees with security training and briefings commensurate with their involvement with classified information.

3-101. Training Materials. Contractors may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

3-102. FSO Training. Contractors shall be responsible for ensuring that the FSO, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements shall be based on the facility's involvement with classified information and may include an FSO orientation course and for FSOS at facilities with safeguarding capability, an FSO Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of FSO.

3-103. Government-Provided Briefings. The CSA is responsible for providing initial security briefings to the FSO, and for ensuring that other briefings required for special categories of information are provided.

3-104. Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, shall be responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using contractor may conduct these briefings.

3-105. Classified Information Nondisclosure Agreement (SF 312). The SF 312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial PCL must execute an SF 312 prior to being granted access to classified information. The contractor shall forward the executed SF 312 to the CSA for retention. If the employee refuses to execute the SF 312, the

contractor shall deny the employee access to classified information and submit a report to the CSA. The SF 312 shall be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

3-106. Initial Security Briefings. Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

- a. A Threat Awareness Briefing.
- b. A Defensive Security Briefing.
- c. An overview of the security classification system.
- d. Employee reporting obligations and requirements.
- e. Security procedures and duties applicable to the employee's job.

3-107. Refresher Training. The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors shall maintain records about the programs offered and employee participation in them. This requirement may be satisfied by use of distribution lists, facility/department-wide newsletters, or other means acceptable to the FSO.

3-108. Debriefings. Contractors shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's PCL is terminated, suspended, or revoked; and upon termination of the FCL.

Chapter 4.

Classification and Marking

Section 1 . Classification

4-100. General. Information is classified pursuant to E.O. 12958 by an original classification authority and is designated and marked as TOP SECRET, SECRET, or CONFIDENTIAL. The designation UNCLASSIFIED is used to identify information that does not require a security classification. Except as provided by statute, (see Chapter 9) no other terms may be used to identify classified information. An original classification decision at any level can be made only by a U.S. Government official who has been delegated the authority in writing. Original classification decisions may require a security classification guide to be issued for use in making derivative classification decisions. Contractors make derivative classification decisions based on the guidance provided by the Contract Security Classification Specification that is issued with each classified contract.

4-101. Original Classification. A determination to originally classify information may be made only when: (a) The information falls into one or more of the categories set forth in E.O. 12958 and (b) The unauthorized disclosure of the information, either by itself or in context with other information, reasonably could be expected to cause damage to the national security that can be identified or described by the original classifier. The original classifier must state the "Reason" for classification on the front page of the document and must also indicate either a date or event for the duration of classification. If the original classifier determines that the classified information falls within one of the categories identified in E.O. 12958 as exempt from automatic declassification, the document will be marked with the appropriate exemption category ("X" code).

4-102. Derivative Classification Responsibilities. Contractors who, extract, or summarize classified information, or who apply classification markings derived from a source document, or as directed by a classification guide or a Contract Security Classification Specification, are making derivative classification decisions. The FSO shall ensure that all employees authorized to perform derivative classification actions are sufficiently trained and that they possess, or have ready access to, the pertinent classification guides and/or guidance necessary to fulfill these important actions. Any specialized training required to implement these responsibilities will be provided by the CSA upon request.

a. The manager or supervisor at the operational level where material is being produced or assembled shall determine the necessity, currency, and accuracy of the classification applied to that material.

b. The manager or supervisor whose signature or other form of approval is required before material is transmitted outside the facility shall determine the necessity, currency, and accuracy of the security classification applied to that material.

c. Individual employees who copy or extract classified information from another document, or who reproduce or translate an entire document, shall be responsible for (1) Marking the new document or copy with the same classification markings as applied to the information or document from which the new document or copy was prepared and (2) Challenging the classification if there is reason to believe the information is classified unnecessarily or improperly.

d. Questions on the classification assigned to reference material are referred as indicated in paragraph 11-206.

e. Commensurate with their involvement, security classification guidance, shall be provided to all employees, including but not limited to, other cleared locations, sales, marketing, technical, production, accounting, clerical, and overseas personnel who have access to classified information in connection with performance on a classified contract.

f. Appropriate security classification guidance shall be provided to subcontractors in connection with classified subcontracts. Subcontractors assume the security classification responsibilities of prime contractors in relation to their subcontractors. (See Chapter 7 for Subcontracting.)

4-103. Security Classification Guidance. The GCA is responsible for incorporating appropriate security requirements clauses in a classified contract and for providing the contractor with the security classification guidance needed during the performance of the contract. This guidance is provided to a contractor by means of the Contract Security Classification Specification. The Contract

Security Classification Specification must identify the specific elements of classified information involved in the contract which require security protection. Contractors shall, to the extent practicable, advise and assist in the development of the original Contract Security Classification Specification. It is the contractor's responsibility to understand and apply all aspects of the classification guidance. Users of classification guides are also encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide. Classification guidance is, notwithstanding the contractor's input, the exclusive responsibility of the GCA, and the final determination of the appropriate classification for the information rests with that activity. The Contract Security Classification Specification is a contractual specification necessary for performance on a classified contract. If a classified contract is received without a Contract Security Classification Specification, the contractor shall advise the GCA.

a. The GCA is required to issue an original Contract Security Classification Specification to a contractor in connection with an IFB, RFP, RFQ, or other solicitation; and with the award of a contract that will require access to, or development of, classified information in the performance of the classified contract.

b. The GCA is required to review the existing guidance periodically during the performance stages of the contract and to issue a revised Contract Security Classification Specification when a change occurs to the existing guidance or when additional security classification guidance is needed by the contractor.

c. Upon completion of a classified contract, the contractor must dispose of the classified information in accordance with Chapter 5, Section 7. If the GCA does not advise to the contrary, the contractor may retain classified material for a period of 2 years following completion of the contract. The Contract Security Classification Specification will continue in effect for this 2-year period. If the GCA determines the contractor has a continuing need for the material, the GCA must issue a final Contract Security Classification Specification for the classified contract. A final specification is provided to show the retention period and to provide final disposition instructions for the classified material under the contract.

4-104. Challenges to Classification. Should a contractor believe (a) That information is classified improperly or unnecessarily; or (b) That current security considerations justify downgrading to a lower classification or upgrading to a higher classification; or (c) That the security classification guidance provided is improper or inadequate, the contractor shall discuss such issues with the pertinent GCA for remedy. If a solution is not forthcoming, and the contractor believes that corrective action is still required, a formal written challenge shall be made to the GCA. Such challenges shall include a description sufficient to identify the issue, the reasons why the contractor believes that corrective action is required, and any recommendations for appropriate corrective action. In any case, the information in question shall be safeguarded as required by this Manual for its assigned or proposed level of classification, whichever is higher, until action is completed. If no written answer is received within 60 days, the CSA should be requested to provide assistance in obtaining a response. If no response is received from the GCA within 120 days, the contractor may also forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) through the Information Security Oversight Office (ISOO). The fact that a contractor has initiated such a challenge will not, in any way, serve as a basis for adverse action by the Government. If a contractor believes that adverse action did result from a classification challenge, full details should be furnished promptly to the ISOO for resolution.

4-105. Contractor Developed Information. Whenever a contractor develops an unsolicited proposal or originates information not in the performance of a classified contract, the following rules shall apply:

a. If the information was previously identified as classified, it shall be classified in accordance with an appropriate Contract Security Classification Specification, classification guide, or source document and marked as required by this Chapter.

b. If the information was not previously classified, but the contractor believes the information may, or should, be classified, the contractor should protect the information as though classified at the appropriate level and submit it to the agency that has an interest in the subject matter for a classification determination. In such a case, the following marking, or one that clearly conveys the same meaning, may be used:

CLASSIFICATION DETERMINATION
PENDING Protect as though classified (TOP SECRET, SECRET, or CONFIDENTIAL).

This marking shall appear conspicuously at least once on the material but no further markings are necessary until a classification determination is received. In addition, contractors are not precluded from marking such material as company-private or proprietary information. Pending a **final** classification determination, the contractor should protect the information. It should be noted however, that E.O.

I 12958 prohibits classification of information over which the Government has no jurisdiction. To be eligible for classification, the information must (1) Incorporate classified information to which the contractor was given prior access, or (2) The Government must first acquire a proprietary interest in the information.

4-106. Classified Information Appearing in **Public Media**. The fact that classified information has been made public does not mean that it is automatically

declassified. Contractors shall continue the classification until formally advised to the contrary. Questions as to the propriety of continued classification in these cases should be brought to the immediate attention of the GCA.

4-107. Downgrading or Declassifying Classified Information. Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. Contractors downgrade or declassify information based on the guidance provided in a Contract Security Classification Specification, upon formal notification, or as shown on the material. These actions constitute implementation of a directed action rather than an exercise of the authority for deciding the change or cancellation of the classification. At the time the material is actually downgraded or declassified, the action to update records and change the classification markings shall be initiated and performed. Declassification, either automatically or by individual review, is not automatically an approval for public disclosure.

Section 2. Marking Requirements

4-200. **General.** Physically marking classified information with appropriate classification markings serves to warn and inform holders of the degree of protection required to protect it. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that **all** classified information and material be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, and any other notations required for protection of the information or material.

4-201. **Marking Requirements for Information and Material.** As a general rule, the markings specified in paragraphs 4-202 through 4-208 are required for all classified information, regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be easily marked with the required markings. Marking other material, such as equipment, AIS media, and slides, will be more difficult due to size or other physical characteristics. Since the principal purpose of the markings is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible to ensure that it is afforded the necessary safeguards.

4-202. **Identification Markings.** All classified material shall be marked to show the name and address of the facility responsible for its preparation, and the date of preparation. These markings are required on the face of all classified documents.

4-203. **Overall Markings.** The highest level of classified information contained in a document is its overall marking. The overall marking shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). If the document does not have a back cover, the outside of the back or last page, which may serve as a cover, may also be marked at the top and bottom with the overall classification of the document. All copies of classified documents shall also bear the required markings. Overall markings shall be stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device. on classified material, other than documents, and on containers of such material, if possible. If marking the material or container is not practical, written notification of the markings shall be furnished to recipients.

4-204. **Page Markings.** Interior pages of classified documents shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, or the designation UNCLASSIFIED, if all the information on the page is UNCLASSIFIED. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page, when necessary to achieve production efficiency, and the particular information to which classification is assigned is adequately identified by portion markings in accordance with 4-206. In any case, the classification marking of a page shall not supersede a lower level of classification indicated by a portion marking applicable to information on that page.

4-205. **Component Markings.** The major components of complex documents are likely to be used separately. In such cases, each major component shall be marked as a separate document. Examples include: (a) each annex, appendix, or similar component of a plan, program, or project description; (b) attachments and appendices to a letter; and (c) each major part of a report. If an entire major component is UNCLASSIFIED, the first page of the component may be marked at the top and bottom with the designation UNCLASSIFIED and a statement included, such as: "All portions of this (annex, appendix, etc.) are UNCLASSIFIED. " When this method of marking is used, no further markings are required on the unclassified major component.

4-206. **Portion Markings.** Each section, part, paragraph, or similar portion of a classified document shall be marked to show the highest level of its classification, or that the portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. For the purpose of applying these markings, a portion or paragraph shall be considered a distinct section or subdivision of a chapter, letter, or document dealing with a particular point or idea which begins on a new line and is often indented. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking portions, the parenthetical symbols (TS) for TOP SECRET, (S) for SECRET, (C) for CONFIDENTIAL, and (U) for UNCLASSIFIED shall be used.

a. Portions of U.S. documents containing foreign government information shall be marked to reflect the foreign country of origin as well as the appropriate classification, for example, (U.K.-C).

b. Portions of U.S. documents containing extracts from NATO documents shall be marked to reflect "NATO" or "COSMIC" as well as the appropriate classification, for example, (NATO-S) or (COSMIC-TS).

c. When illustrations, photographs, figures, graphs, drawings, charts, or similar portions are contained in classified documents they shall be marked clearly to show their classified or unclassified status. These classification markings shall not be abbreviated and shall be prominent and placed within or contiguous (touching or near) to such a portion. Captions of such portions shall be marked on the basis of their content alone by placing the symbol (TS), (S), (C), or (U) immediately preceding the caption.

d. If, in an exceptional situation, parenthetical marking of the portions is determined to be impractical, the classified document shall contain a description sufficient to identify the exact information that is classified and the classification level(s) assigned to it. For example, each portion of a document need not be separately marked if all portions are classified at the same level, provided a full explanation is included in the document.

4-207. **Subject and Title Markings.** Unclassified subjects and titles shall be selected for classified documents, if possible. An unclassified subject or title shall be marked with a (U) placed immediately following and to the right of the item. A classified subject or title shall be marked with the appropriate symbol (TS), (S), or (C) placed immediately following and to the right of the item.

4-208. **Markings for Derivatively Classified Documents.** All classified information shall be marked to reflect the source of the classification and declassification instructions. The markings used to show this information are as follows:

DERIVED FROM _____
DECLASSIFY ON _____

Documents shall show the required information either on the cover, first page, title page, or in another prominent position. Other material shall show the

required information on the material itself or, if not practical, in related or accompanying documentation.

a. **"DERIVED FROM" Line.** The purpose of the "Derived From" line is to link the derivative classification applied to the material by the contractor and the source document(s) or classification guide(s) under which it was classified. In completing the "Derived From" line, the contractor shall identify the applicable guidance that authorizes the classification of the material. Normally this will be a security classification guide listed on the Contract Security Classification Specification or a source document. When identifying a classification guide on the "Derived From" line, the guide's title or number, issuing agency, and date shall be included. Many Contract Security Classification Specifications cite more than one classification guide and/or the contractor is extracting information from more than one classified source document. In these cases, the contractor may use the phrase "multiple sources." When the phrase "multiple sources" is used, the contractor shall maintain records that support the classification for the duration of the contract under which the material was created. These records may take the form of a bibliography identifying the applicable classification sources and be included in the text of the document or they may be maintained with the file or record copy of the document. When practical, this information should be included in or with all copies of the derivatively classified document. If the only source for the derivative classification instructions is the Contract Security Classification Specification, the date of the Contract Security Classification Specification and the specific contract number for which it was issued shall be included on the "Derived From" line.

b. **"DECLASSIFY ON" Line.** The purpose of the "Declassify On" line is to provide declassification instructions appropriate for the material. When completing this line, the contractor shall use the information specified in the Contract Security Classification Specification or classification guide furnished with a classified contract or carry forward the duration instruction from the source document or classification guide (e.g., date, event, or "X" code). When the source is marked "Original Agency's Determination Required" (OADR), the "Declassify On" line should show: "Source Marked OADR, Date of Source (MM/DD/YY)." When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its

sources. Material containing Restricted Data or Formerly Restricted Data shall not have a "Declassify On" line.

c. **"DOWNGRADE TO" Line.** When downgrading instructions are contained in the Contract Security Classification Specification, classification guide, or source document, a "Downgrade To" line will be included. When completing this line, the contractor shall insert SECRET or CONFIDENTIAL and an effective date or event. The markings used to show this information are as follows:

DERIVED FROM _____
DOWNGRADE TO _____ O N _
DECLASSIFY ON _____

d. **"CLASSIFIED BY" Line and "REASON CLASSIFIED" Line.** As a general rule, a "Classified By" line and a "Reason Classified" line will only be shown on originally classified documents. However, certain agencies may require that derivatively classified documents contain a "Classified By" line to identify the derivative classifier and a "Reason Classified" Line to identify the specific reason for the derivative classification. Instructions for the use of these lines will be included in the security classification guidance provided with the contract.

4-209. **Extracts of Information.** Most classified material originated under recent Executive orders contains overall, portion, paragraph, and appropriate downgrading and declassification markings that will provide sufficient guidance for the classification of extracted information. However, some classified material may not have these markings. If contractors encounter source documents that do not provide the needed markings the following procedures apply.

a. Information extracted from a classified source document shall be classified according to the classification markings on the source.

(1) If the source document contains portion markings, the classification of the extracted portions shall be carried forth to the new material.

(2) If the source document does not contain portion markings, the overall classification of the source document shall be carried forth to the extracted information in the new document.

(3) If the new material is classified based on "multiple sources," the highest level of classification contained in the document shall be shown as the overall classification on the new material.

b. Downgrading and declassification markings shown on the source shall be carried forth to the new material.

(1) If only one source is used, the downgrading and declassification markings shown on the source shall be carried forward to the new material. If no date, event, or "X" code is shown on the source and the source is marked "OADR," the new material shall show "Source Marked OADR" and the date of the source document shall be identified on the "Declassify On" line.

(2) If the new material is classified based on "multiple sources," the longest duration date or event, or "X" code shown on any source shall be assigned to the new material. If any source shows "OADR," the "Declassify On" line on the new document shall show "Source Marked OADR" and the date of the most recent source document.

c. If the contractor requires more definitive guidance, the originator of the source document, or the GCA that provided the document, may be contacted and requested to provide appropriate markings or an appropriate security classification guide. In any case, the classification markings for a source document are the responsibility of the originator, and not the contractor extracting the information. Contractors are encouraged to contact the originator to avoid improper or unnecessary classification of material.

4-210. **Marking Special Types of Material.** The following procedures are for marking special types of material, but are not all inclusive. The procedures cover the types of materials that are most often produced by contractors and may be varied to accommodate [he physical characteristics of the material, organizational and operational requirements, and ultimate use of the item produced. The intent of the markings is to ensure that the classification of the item, regardless of its form, is clear to the holder.

a. **Files, Folders, or Groups of Documents.** Files, folders, binders, envelopes, and other items, containing classified documents, when not in secure storage, shall be conspicuously marked with the

highest classification of any classified item included therein. Cover sheets may be used for this purpose.

b. Messages Electronically transmitted messages shall be marked in the same manner required for other documents except as noted herein. The overall classification of the message shall be the first item of information in the text. A "Derived From" line is required on messages. Certain agencies may also require that messages contain a "Classified By" and a "Reason Classified" line in order to identify the derivative classifier and the specific reason for classification. Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents. When messages are printed by an automated system, all markings may be applied by that system, provided the classification markings are clearly distinguished from the printed text. The last line of text of the message shall include the declassification instructions. In record communications systems, electronically transmitted messages shall be marked in accordance with JANAP 128 format requirements.

c. Microforms. Microforms contain images or text in sizes too small to be read by the unaided eye. The applicable markings specified in 4-202 through 4-208 shall be conspicuously marked on the microform medium or its container, to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Further markings and handling shall be as appropriate for the particular microform involved.

d. Translations. Translations of U.S. classified information into a language other than English shall be marked to show the U.S. as the country of origin, with the appropriate U.S. markings as specified in 4-202 through 4-208, and the foreign language equivalent thereof. (See Appendix B).

4-211. **Marking Transmittal Documents.** A transmittal document shall be marked with the highest level of classified information contained therein and with an appropriate notation to indicate its classification when the enclosures are removed. An unclassified document that transmits a classified document as an attachment shall bear a notation substantially as follows: Unclassified when Separated from Classified Enclosures. A classified transmittal that transmits higher classified information shall be marked with a notation substantially as follows:

CONFIDENTIAL (or SECRET) when Separated from Enclosures. In addition, a classified transmittal itself must bear all the classification markings required by this Manual for a classified document.

4-212. **Marking Wholly Unclassified Material.** Normally, wholly UNCLASSIFIED material will not be marked or stamped UNCLASSIFIED unless it is essential to convey to a recipient of such material that: (a) The material has been examined specifically with a view to impose a security classification and has been determined not to require classification; or (b) The material has been reviewed and has been determined to no longer require classification and it is declassified.

4-213. **Marking Compilations.**

a. Documents. In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document. In this instance, the portions of a document classified in this manner need not be marked.

b. Portions of a Document. If a classified document contains certain portions that are unclassified when standing alone, but classified information will be revealed when they are combined or associated, those portions shall be marked as unclassified, the page shall be marked with the highest classification of any information on the page, and a statement shall be added to the page, or to the document, to explain the classification of the combination or association to the holder. This method of marking may also be used if classified portions on a page, or within a document, will reveal a higher classification when they are combined or associated than when they are standing alone.

4-214. **Marking Miscellaneous Material.** Unless a requirement exists to retain material such as rejects, typewriter ribbons, carbons, and similar items for a specific purpose, there is no need to mark, stamp, or otherwise indicate that the material is classified. (NOTE: Such material developed in connection with the handling, processing, production, and utilization

of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and destruction at the earliest practical time.)

4-215. **Marking Training Material.** Unclassified documents or material that are created to simulate or demonstrate classified documents or material shall be clearly marked to indicate the actual UNCLASSIFIED status of the information. For example: SECRET FOR TRAINING PURPOSES ONLY, OTHERWISE UNCLASSIFIED or UNCLASSIFIED SAMPLE, or a similar marking may be used.

4-216. Marking Downgraded or Declassified Material. Classified information, which is downgraded or declassified, shall be promptly and conspicuously marked to indicate the change. If the volume of material is such that prompt remarking of each classified item cannot be accomplished without unduly interfering with operations, a downgrading and declassification notice may be attached to the inside of the file drawers or other storage container in lieu of the remarking otherwise required. Each notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage container to which it applies. When documents or other material subject to downgrading or declassification are withdrawn from the container solely for transfer to another, or when the container is transferred from one place to another, the transfer may be made without remarking, if the notice is attached to the new container or remains with each shipment. When the documents or material are withdrawn for use or for transmittal outside the facility, they shall be remarked in accordance with a or b below.

a. Automatic Downgrading or Declassification Actions. Holders of classified material may take automatic downgrading or declassification actions as specified by the markings on the material without further authority for the action. All old classification markings shall be canceled and the new markings substituted, whenever practical. In the case of documents, as a minimum, the outside of the front cover (if any), the title page (if any), the first page, and the outside of the back cover (if any), shall reflect the new classification markings, or the designation UNCLASSIFIED. Other material shall be remarked by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to

the material. Old markings shall be canceled, if possible, on the material itself. If not practical, the material may be marked by affixing new decals, tags, stickers, and the like to the material or its container.

b. Other than Automatic Downgrading or Declassification Actions. When contractors are notified of downgrading or declassification actions that are contrary to the markings shown on the material, the material shall be remarked to indicate the change. All old classification markings shall be canceled and the new markings substituted, whenever practical. In the case of documents, as a minimum, the outside of the front cover (if any), the title page (if any), the first page, and the outside of the back cover (if any), shall reflect the new classification markings or the designation UNCLASSIFIED. In addition, the material shall be marked to indicate the authority for the action, the date of the action, and the identity of the person or contractor taking the action. Other holders shall be notified if further dissemination has been made by the contractor.

4-217. **Upgrading Action.** When a notice is received to upgrade material to a higher level, for example from CONFIDENTIAL to SECRET, the new markings shall be immediately entered on the material in accordance with the notice to upgrade, and all the superseded markings shall be obliterated. The authority for, and the date of, the upgrading action shall be entered on the material. As appropriate, other holders shall be notified if further dissemination of the material has been made by the contractor. (See 4-218 below).

4-218. **Miscellaneous Actions.** If classified material is inadvertently distributed outside the facility without the proper classification assigned to it, or without any markings to identify the material as classified, the contractor shall, as appropriate:

a. Determine whether all holders of the material are cleared and are authorized access to it.

b. Determine whether control of the material has been lost.

c. If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If control of the material has been lost, if all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to the CSA.

d. In the case of classified material being upgraded, the contractor's written notice **shall** not be classified unless the notice contains additional information warranting classification. In the case of material which was inadvertently released as UNCLASSIFIED, the contractor's written notice shall be classified CONFIDENTIAL, unless it contains additional information warranting a higher classification. The notice shall cite the applicable Contract Security Classification Specification or other classification guide on the "Derived From" line and be marked with an appropriate declassification instruction.

4-219. Documents Generated Under Previous Executive Orders. Documents classified under

previous executive orders need not be remarked to comply with the marking requirements of E.O. 12958. Any automatic downgrading or declassification action specified on such documents may be taken without further authority. Information extracted from these documents for use in new documents shall be marked for downgrading or declassification action as specified on the source document. If automatic downgrading or declassification markings are not included on the source documents, the documents shall remain classified until authority is obtained from the originating agency for downgrading or declassification action. Information extracted from such documents for use in new documents shall conform to the marking requirements of this chapter.

Section 2. Control and Accountability

5-200. General. Contractors shall establish an information management system and control the classified information in their possession.

5-201. Policy. The document accountability system for SECRET material is eliminated as a security protection measure, except for highly sensitive program information and where special conditions exist as approved by the GCA. Contractors shall ensure that classified information in their custody is used or retained only in furtherance of a lawful and authorized U.S. Government purpose. The U.S. Government reserves the right to retrieve its classified material or to cause appropriate disposition of the material by the contractor. The information management system employed by the contractor shall be capable of facilitating such retrieval and disposition in a reasonable period of time.

5-202. External Receipt and Dispatch Records. Contractors shall maintain a record that reflects: (a) The date of the material; (b) The date of receipt or dispatch; (c) The classification; (d) An unclassified description of the material; and (e) The identity of the activity from which the material was received or to which the material was dispatched. Receipt and dispatch records shall be retained for 2 years.

5-203. **Accountability for TOP SECRET.**

a. TOP SECRET control officials shall be designated to receive, transmit, and maintain access and accountability records for TOP SECRET information. An inventory shall be conducted annually unless written relief is granted by the GCA.

b. The transmittal of TOP SECRET information shall be covered by a continuous receipt system both within and outside the facility.

c. Each item of TOP SECRET material shall

be numbered in series. The copy number shall be placed on TOP SECRET documents and on all associated transaction documents.

5-204. **Receiving Classified Material.** All classified material shall be delivered directly to designated personnel. When U.S. Registered Mail, U.S. Express Mail, U.S. Certified Mail, or classified material delivered by messenger is not received directly by designated personnel, procedures shall be established to ensure that the material is received by authorized persons for prompt delivery or notice to authorized personnel. The material shall be examined for evidence of tampering and the classified contents shall be checked against the receipt. Discrepancies in the contents of a package, or absence of a receipt for TOP SECRET and SECRET material, shall be reported promptly to the sender. If the shipment is in order, the receipt shall be signed and returned to the sender.. If a receipt is included with CONFIDENTIAL material, it shall be signed and returned to the sender.

5-502. **Generation of Classified Material.**

a. A record of TOP SECRET material produced by the contractor shall be made when the material is: (1) Completed as a finished document; (2) Retained for more than 30 days after creation, regardless of the stage of development; or (3) Transmitted outside the facility.

b. Classified working papers generated by the contractor in the preparation of a finished document shall be: (1) Dated when created; (2) Marked with its overall classification, and with the annotation, "WORKING PAPERS;" and (3) Destroyed when no longer needed. Working papers shall be marked in the same manner prescribed for a finished document at the same classification level when: (1) Transmitted outside the facility; or (2) Retained for more than 180 days from creation.

Chapter 9

Special Requirements

Section 1. Restricted Data and Formerly Restricted Data

9-100. General. This Section contains information and the requirements for safeguarding atomic energy information that is designated “Restricted Data” and “Formerly Restricted Data.” Such information is classified under the authority of the Atomic Energy Act of 1954 and is under the jurisdiction and control of the Department of Energy (DOE). For purposes of this Section, a distinction is made between National Security Information and atomic energy information as explained below.

9-101. Authority and Responsibilities.

a. The Atomic Energy Act of 1954, as amended, provides for the development, use, and control of atomic energy. The Act establishes policy for handling atomic energy-related classified information designated as Restricted Data (RD) and Formerly Restricted Data (FRD). The Act provides responsibility to DOE to “control the dissemination and declassification of Restricted Data.” In Section 143 of the Act, the Secretary of Defense has the responsibility to establish personnel and other security procedures and standards that are in reasonable conformity to the standards established by the Department of Energy. This Section is intended to ensure reasonable conformity in policy and procedures used by contractors for the control of RD and FRD.

b. The Secretary of Energy and the Chairman of the Nuclear Regulatory Commission retain authority over access to information which is under their respective cognizance as directed by the Atomic Energy Act of 1954. The Secretary or the Commission may inspect and monitor contractor programs or facilities that involve access to such information or may enter into written agreement with the DOD to inspect and monitor these programs or facilities.

9-102. Background Information.

a. The Atomic Energy Act is the basis for classification of atomic energy information as Restricted Data and Formerly Restricted Data. In accordance with the Atomic Energy Act, all atomic energy information is classified unless a positive action is taken to declassify it. This is directly opposite to procedures used for information classified

by E.O. 12958. This is a significant difference that should be clearly understood. By the Act, Congress has decreed that atomic energy information is different -- it is “born classified,” it remains classified until a positive action is taken to declassify it, and it may be declassified only by the Department of Energy. No other organization can declassify atomic energy information, and once it is declassified, it cannot be reclassified.

b. “Restricted Data” (RD) is defined in the Atomic Energy Act as follows:

“The term Restricted Data means all data concerning, (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142.”

c. “Formerly Restricted Data” (FRD) is information which has been removed from the Restricted Data category after the DOE and the DOD have jointly determined that the information relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as National Security Information in the United States. Such data may not be given to any other nation except under specially approved agreements and with the authorization of DOE. FRD is identified and handled as Restricted Data when sent outside the United States.

9-103. Unauthorized Disclosures Contractors shall report all unauthorized disclosures involving RD and FRD to the DOE or NRC through their CSA.

9-104. International Requirements. The Act provides for a program of international cooperation to promote common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit. Information controlled by the Ac[may be shared with another nation only under the terms of an agreement for cooperation. The disclosure by a contractor of RD and FRD shall not be permitted until an agreement is signed by the United States and participating governments and disclosure guidance and security

arrangements are established. RD and FRD shall not be transmitted to a foreign national or regional defense organization unless such action is approved and undertaken pursuant to an agreement for cooperation between the United States and the cooperating entity and supporting statutory determinations as prescribed in the Act.

9-105. **Personnel Security Clearances. Only** DOE, NRC, DoD, and NASA can grant access to RD and FRD. Contractors of all other federal agencies must be processed for PCLS by the DOE. The minimum investigative requirements and standards for access to RD and FRD are set forth below.

a. Top Secret RD-A favorable Single Scope Background Investigation (SSBI).

b. Secret RD-A favorable SSBI. (SRD as defined pursuant to the NISPOMSUP).

c. Confidential RD-A favorable NACLC.

d. Top Secret FRD-A favorable SSBI.

e. Secret FRD-A favorable NACLC.

f. Confidential FRD-A favorable NACLC.

DOE and NRC use the designation Q when a favorable access authorization determination has been conducted based on an SSBI and L when a favorable access authorization determination has been made based on an NACLC.

9-106. Classification.

a. Since RD is born classified, no classification category determination by a person with original classification authority is ever required for RD or FRD; however, an authorized classifier must determine the classification level. No date or event for automatic declassification ever applies to RD or FRD.

b. Only RD Classifiers appointed and trained under Government Agency procedures may derivatively classify material that contains RD. Any contractor employee authorized to derivatively classify NSI material may also derivatively classify FRD material. Such derivative classification determinations shall be based on classification guidance approved by the DOE or NRC and not on portion markings in a source document. If such classification guidance is not available and the

information in the document meets the definition of RD, then the classifier shall, as an interim measure, mark the document as Confidential RD or, if the sensitivity of the information in the document so warrants, as Secret RD. Such document shall be promptly referred to the CSA who shall provide the contractor with the **final** determination based upon official published classification guidance.

c. RD and FRD are not limited to U.S. Government information. Contractors who develop RD, FRD, or an invention or discovery useful in the production or utilization of special nuclear material or atomic energy shall file a report with a complete description thereof with the DOE or the Commissioner of Patents as prescribed by the Act. Documents thought to contain RD or FRD shall be marked temporarily as such. Such documents shall be promptly referred to the CSA for a final determination based upon official published classification guidance.

9-107. **Declassification.** Documents marked as containing RD and FRD remain classified until a positive action by an authorized person is taken to declassify them; no date or event for automatic declassification ever applies to RD and FRD documents. Only the DOE may declassify contractor documents marked as RD. Only the DOE or the DOD may declassify contractor documents marked as FRD. These authorities may be delegated on a case-by-case basis. Contractors shall send any document marked as RD or FRD that must be declassified or sanitized to the appropriate government contracting office.

9-108. **Transclassification.** Transclassification occurs when information is removed from the RD category by a joint determination of DOE and DOD and placed in the FRD category in accordance with section 142d of the Atomic Energy Act. This information is primarily related to the military utilization of atomic weapons and can be adequately safeguarded as NSI. This authority is severely restricted and cannot be exercised by RD Classifiers. Contact the DOE for information.

9-109. Marking. In addition to the markings specified in Chapter 4 for NSI, classified material containing RD and FRD shall be marked as indicated below:

a. Restricted Data. The following notice shall be affixed on material that contains Restricted Data. This may be abbreviated RD.

Restricted Data

This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

Material classified as RD must indicate the classification guide and the authorized RD classifier. The following marking shall be applied:

Classified by: (guide)

Classifier: (name and title)

b. Formerly Restricted Data. The following notice shall be affixed on material which contains Formerly Restricted Data, This may be abbreviated FRD.

Formerly Restricted Data

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, AEA 1954.

Material classified as FRD must indicate the classification guide. The following marking shall be applied:

Classified by: (guide)

c. Documents shall be marked to indicate CNWDI, Sigmas, and NNPI, as applicable.

9-110. Automated Information Systems. See the NISPOMSUP for AIS requirements for TSRD and SRD.

9-111. Physical Security. See the NISPOMSUP for physical security requirements for TSRD and SRD.

Section 3. Foreign Government Information

10-300. General. Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. This Section provides additional requirements for protecting and controlling access to foreign government information provided to U.S. contractors.

10-301. Policy. The contractor shall notify the CSA when awarded contracts by a foreign interest that will involve access to classified information. The CSA shall administer oversight and ensure implementation of the security requirements of the contract on behalf of the foreign government, including the establishment of channels for the transfer of classified material.

10-302. Marking Foreign Government Classified Material. Foreign government designations for classified information generally parallel U. S. security classification designations. However, some foreign governments have a fourth level of classification, RESTRICTED, for which there is no equivalent U.S. classification. The information is to be protected and marked as CONFIDENTIAL information. When other foreign government material is received, the equivalent U.S. classification and the country of origin shall be marked on the front and back in English. Foreign government classification designations and the U.S. equivalents are shown in Appendix B.

10-303. Marking U.S. Documents That Contain Foreign Government Information.

a. U.S. documents that contain foreign government information shall be marked on the front, "THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION." In addition, the portions shall be marked to identify both the country and classification level, e.g., (UK-C); (GE-C). The "Derived From" line shall identify U.S. as well as foreign classification sources.

b. If the identity of the foreign government must be concealed, the front of the document shall be marked "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION," paragraphs shall be marked FGI, together with the classification level, e.g., (FGI-C), and the "Derived From" line shall indicate FGI in addition to any U.S. source. The identity of the foreign government shall be maintained with the record copy of the document.

c. A U.S. document, marked as described herein, shall not be downgraded below the highest level of foreign government information contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification shall be submitted to the GCA or foreign government contracting authority, as applicable.

10-304. Marking Documents Prepared For Foreign Governments. Documents prepared for foreign governments that contain U.S. and foreign government information shall be marked as prescribed by the foreign government. In addition, they shall be marked on the front, "THIS DOCUMENT CONTAINS UNITED STATES CLASSIFIED INFORMATION." Portions shall be marked to identify the U.S. classified information. The record specified in paragraph 10-204b shall be maintained.

10-305. PCL, FCL, and Briefing Requirements. PCLS and FCLS issued by the U.S. Government are valid for access to classified foreign government information of a corresponding level. Contractor employees will be briefed and acknowledge in writing their responsibilities for handling foreign government information prior to being granted access.

10-306. Storage, Control, and Accountability. Foreign government material shall be stored and access controlled generally in the same manner as U.S. classified material of an equivalent classification. The procedures shall ensure that the material can be located at all times and access is limited to only those persons who require access for the specific purpose for which the information was provided by the originating government. Foreign government material shall be stored in a manner that will avoid commingling with other material which may be accomplished by establishing separate files in a storage container. Annual inventories are required for TOP SECRET and SECRET material.

10-307. **Disclosure and Use Limitations.** Foreign government information shall not be disclosed to nationals of a third country, including intending citizens, or to any other third party, or be used for other than the purpose for which it was provided, without the prior written consent of the originating foreign government. Requests for other uses or further disclosure shall be submitted to the GCA for U.S. contracts, and through the CSA for direct commercial contracts. Approval of the request does

not alleviate the requirement for the contractor to obtain an export authorization.

10-308. Exports of Foreign Government Information. An export authorization is required for the export or **re-export** of export-controlled foreign government information except for technical data being returned to the original source of import. All requests for export authorization for foreign government information shall clearly identify and distinguish between the foreign government information and any U.S. information involved in the same request. Foreign government information shall not be exported to a third party without the prior consent of the originating government. A copy of such consent shall be provided in writing to the Office of Defense Trade Controls, Department of State, with an information copy to the **CSA**.

10-309. Transfer. Foreign government information shall be **transferred** within the U. S., its possessions, or territories, using the same channels as specified by this Manual for U.S. classified information of an equivalent classification except that uncleared commercial delivery services shall not be used. The transfer of foreign government information to areas outside the U.S. shall be through government-to-government channels

10-310. Contract Security Requirements. The foreign entity that awards a classified contract is responsible for providing appropriate security classification guidance and any security requirements clauses. The failure of a foreign entity to provide classification guidance shall be reported to the **CSA**.

10-311. Public Disclosure. The public disclosure of foreign government information requires the prior written approval of the contracting foreign government.

10-312. Subcontracting.

a. A U.S. contractor may award a subcontract that involves access to foreign government information to another contractor within the U. S., its possessions or territories, except as described in subparagraph b, below, upon verifying with the **CSA** that the prospective subcontractor has

the appropriate FCL and storage capability. The contractor awarding a subcontract shall provide appropriate security classification guidance and incorporate the pertinent security requirements clauses in the subcontract.

b. Subcontracts involving foreign government information shall not be awarded to a contractor in a third country or to a U.S. company with a limited FCL based on third-country ownership, control, or influence without the express written consent of the originating foreign government. The **CSA** will coordinate with the appropriate foreign government authorities to resolve the matter.

10-313. Reproduction. The reproduction of foreign government TOP SECRET information requires the written approval of the originating government. Reproduced copies of all foreign government information shall be controlled, protected, and accounted for in the same manner as the original version.

10-314. Disposition. Foreign government information shall be returned to the **GCA** or foreign government that provided the information, upon completion of the contract, unless the contract specifically authorizes destruction or retention of the information. TOP SECRET and SECRET destruction must be witnessed; destruction certificates are required for foreign government material and shall be retained for 3 years.

10-315. Loss, Compromise, or Suspected Compromise. The loss, compromise, or suspected compromise of foreign government material shall be reported promptly to the **CSA**.

10-316. Reporting of Improper Receipt of Foreign Government Material. The contractor shall report to the **CSA** the receipt of classified material from foreign interests that is not received through government channels.

10-317. Processing Foreign Government Classified Information on AISS. Foreign government information shall be processed on an AIS accredited to the appropriate classification level.

Section 3. Independent Research and Development Efforts

11-300. General. This Section provides special procedures and requirements necessary for safeguarding classified information when it is incorporated in contractors independent research and development (IR&D) efforts.

11-301. Limitations. Contractors frequently must use classified information in their IR&D efforts to effectively explore technological advancements and state-of-the-art improvements.

a. Contractors are generally precluded from disclosing classified information to other cleared contractors in connection with an IR&D effort without the prior written approval of the agency that has jurisdiction over the information or the agency that provided the information to the contractor.

b. DoD contractors shall not release or disclose classified information, under the jurisdiction of a non-DoD Agency to other cleared contractors in connection with an IR&D effort without the written approval of the non-DoD Agency.

c. DoD cleared contractors may disclose SECRET and CONFIDENTIAL information, under the jurisdiction of a DoD contracting activity, to other DoD cleared contractors in connection with an IR&D effort unless specifically prohibited by the DoD in a Contract Security Classification Specification or other written notification.

11-302. Information Generated Under an IR&D Effort that Incorporates Classified Information.

Under E.O. 12958, information that is in substance the same as information currently classified, requires a derivative classification. Therefore, information in a contractor's IR&D effort will require a derivative classification.

11-303. Classification Guidance. The releasing contractor may extract guidance appropriate for the IR&D effort from:

a. An existing Contract Security Classification Specification that was previously

furnished by a GCA in connection with performance of a classified contract:

b. A final Contract Security Classification Specification that was issued in connection with retention of classified documents under a completed contract;

c. A security classification guide obtained from DTIC;

d. A classified source document.

NOTE: The Department of Defense "Index of Security Classification Guides," and many of the listed security classification guides, are available to contractors who are registered with the DTIC. Contractors are encouraged to use the Index and the listed guides to obtain up-to-date security guidance for the classified information involved when developing guidance appropriate for their IR&D efforts.

11-304. Preparation of Security Guidance. Contractors shall use the Contract Security Classification Specification to provide security guidance for the classified information released in their IR&D efforts.

11-305. Retention of Classified Documents Generated Under IR&D Efforts. Contractors may retain the classified documents that were generated in connection with their classified IR&D efforts for the duration of their facility clearance provided they have proper storage capability. Documents shall be clearly identified as "IR&D DOCUMENTS." A contractor's facility clearance will not be continued solely for the purpose of retention of classified IR&D documents without specific retention authorization from the GCA that has jurisdiction over the classified information contained in such documents. Contractors shall establish procedures for review of their IR&D DOCUMENTS on a recurring basis to reduce their classified inventory to the minimum necessary.

Appendix C.

Definitions

Access. The ability and opportunity to obtain knowledge of classified information.

Adverse Information. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

Affiliate. Any entity effectively owned or controlled by another entity.

Approved Access Control Device. An access control device that meets the requirements of this Manual as approved by the FSO.

Approved Built-in Combination Lock. A combination lock, equipped with a top-reading dial, that conforms to Underwriters' Laboratories, Inc. Standard Number, UL 768, Group 1R.

Approved Combination Padlock. A three-position dial-type changeable combination padlock listed on the GSA Qualified Products List as meeting the requirements of Federal Specification FF-P- 110.

Approved Electronic, Mechanical, or Electro-mechanical Device. An electronic, mechanical, or electro-mechanical device that meets the requirements of this Manual as approved by the FSO.

Approved Key-Operated Padlock. A padlock, which meets the requirements of MIL-SPEC-P-43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), National Stock Number 5340-00-799-8016,

Approved Security Container. A security file container, originally procured from a Federal Supply Schedule supplier that conforms to federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock. Such containers will be labeled "General Services Administration Approved Security Container" on the face of the top drawer. Acceptable tests of these containers can be performed only by a testing facility specifically approved by GSA.

Approved Vault. A vault that has been constructed in accordance with this Manual and approved by the CSA.

Approved Vault Door. A vault door and frame unit originally procured from the Federal Supply Schedule (FSC Group 71, Part III, Section E, FSC Class 7110), that meets Federal Specification AA-D-600.

Authorized Person. A person who has a need-to-know for classified information in the performance of official duties and who has been granted a personnel clearance at the required level.

Automated Information System. An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Automated Information System Security. All security safeguards needed to provide an acceptable level of protection for Automated Information Systems and the classified data processed.

Classification Authority. The authority that is vested in a government official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

Classified Contract. Any contract that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a "classified contract" also are applicable to all phases of precontract activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.

Classification Guide. A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specific information [to be classified on a derivative basis. (Classification guides are

provided to contractors by the Contract Security Classification Specification.)

Classified Information. The term includes National Security Information, Restricted Data, and Formerly Restricted Data.

Classified Information Procedures Act. A law that provides a mechanism for the courts to determine what classified information the defense counsel may access.

Classified Visit. A visit **during** which the visitor will require, or is expected to require, access to classified information.

Classifier. Any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or it may be a derivative classification action. Contractors make derivative classification determinations based on classified source material, a security classification guide, or a Contract Security Classification Specification.

Cleared Commercial Carrier. A carrier that is authorized by law, regulatory body, or regulation to transport SECRET material and has been granted a SECRET facility clearance.

Cleared Employees. All **contractor employees granted a personnel security clearance (PCL) and all employees in-process for a PCL.**

Closed Area. An area that meets the requirements of this Manual, as approved by the CSA, for the purpose of safeguarding classified material that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

Cognizant Security Agency. Agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. The Secretary of Defense (SECDEF) has been designated as Executive Agent for the NISP. Heads of the Executive Branches are required to enter into agreements with the SECDEF that establish the terms of the SECDEF's

responsibilities on behalf of these agency heads for administration of industrial security on their behalf.

Cognizant Security Office. The office or offices delegated by the Head of a CSA to administer industrial security in a contractor's facility on behalf of the CSA.

Colleges and Universities All educational institutions that award academic degrees, and related research activities directly associated with a college or university through organization or by articles of incorporation.

Communications Intelligence. Technical and intelligence information derived from foreign communications by other than the intended recipient.

Communications Security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.

Company. A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to commonly prosecute a commercial, industrial or other legitimate business, enterprise, or undertaking.

Compromise. The disclosure of classified information to an unauthorized person.

CONFIDENTIAL. The designation that shall be applied to information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security that the original classification authority is able to identify or describe.

Consignee. A person, firm, or government activity named as the receiver of a shipment; one to whom a shipment is consigned.

Consignor. A **person,** firm, or government activity by whom articles are shipped. The consignor is usually the shipper.

Constant Surveillance Service. A transportation protective service provided by a commercial carrier qualified by MTMC to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative, however, a facility clearance is not required for the carrier. The carrier providing the

service must maintain a signature and tally record for the shipment.

Continental Limits of the United States. U.S. territory, including the adjacent territorial waters located within the North American continent between Canada and Mexico.

Contracting Officer. A government official who, in accordance with departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

Contractor. Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

Courier. A cleared employee, designated by the contractor, whose principal duty is to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

Conversion Rights. The right inherent in the ownership or holding of particular securities to exchange such securities for voting securities.

Critical Nuclear Weapon Design Information. A DoD category of weapon data designating TOP SECRET Restricted Data or SECRET Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device.

Custodian. An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.

Declassification. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

Declassification Event. An event that eliminates the need for continued classification of information.

Defense Transportation System. Military controlled terminal facilities, Military Airlift Command

controlled aircraft, Military Sealift Command controlled or arranged sealift and Government controlled air or land transportation.

Department of Defense. The Office of the Secretary of Defense (OSD) (including all boards, councils, staffs, and commands), DoD agencies, and the Departments of Army, Navy, and Air Force (including all of their activities).

Derivative Classification. A determination that information is in substance the same as information currently classified and the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. Persons who apply derivative classification markings shall observe and respect original classification decisions and carry forward to any newly created documents any assigned authorized markings.

Document. Any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

Downgrade. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

Effectively Owned or Controlled. A foreign government or any entity controlled by a foreign government has the power, either directly or indirectly, whether exercised or exercisable, to control the election, appointment or tenure of the Offeror's officers, or a majority of the Offeror's board of directors by any means; e.g., ownership, contract, or operation of law (or equivalent power for unincorporated organizations).

Embedded System. An AIS that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem such as, ground support equipment, flight simulators, engine test stands, or fire control systems.

Entity. Any U.S. or foreign person.

Escort. A cleared employee, designated by the contractor, who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort,

Evaluated Products List. A documented inventory of equipments, hardware software, and/or firmware that have been evaluated against the evaluation criteria found in DoD 5200.28 -STD.

Facility. A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.

Facility (Security) Clearance. An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

Firmware. A method of organizing control of an AIS in a microprogrammed structure in addition to, or rather than, software or hardware. Microprograms are composed of microinstruction, normally resident in read-only memory, to control the sequencing of computer circuits directly at the detailed level of the single machine instruction.

Foreign Government. Any national governing body organized and existing under the laws of any country other than the United States and its possessions and trust territories and any agent or instrumentality of that government.

Foreign Government Information. Information that is: a. Provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or b. Produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments or any

element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

Foreign Interest. Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the U.S. or its possessions and trust territories, and any person who is not a citizen or national of the United States.

Foreign Nationals. Any person who is not a citizen or national of the United States.

Foreign Person. Any foreign interest and any U.S. person effectively owned or controlled by a foreign interest.

Foreign Recipient. A foreign government or international organization, to whom the U.S. is providing classified material.

Formerly Restricted Data. Classified information jointly determined by the DOE and its predecessors and the DOD to be related primarily to the military utilization of atomic weapons and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

Freight Forwarder (Transportation Agent). Any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of this Manual, an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

Government-To-Government Channels. Transfers by government officials through official channels or through other channels specified by the governments involved.

Government Contracting Activity. An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Handcarrier. A cleared employee, designated by the contractor, who occasionally handcarries classified material to its destination in connection with a classified visit or meeting. The classified material

remains in the personal possession of the handcarrier except for authorized overnight storage.

Home Office Facility. The headquarters facility of a multiple facility organization.

Independent Research and Development. A contractor funded research and development effort that is not sponsored by, or required in performance of, a contract or grant that consists of projects falling with the areas of basic research; applied research; development; and systems, and other concept formulation studies.

Industrial Security. That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry.

Information. Any information or material, regardless of its physical form or characteristics.

Information Security. The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.

Information Systems Security Representative. The contractor employee responsible for the implementation of Automated Information Systems security, and operational compliance with the documented security measures and controls, at the contractor facility.

Intelligence. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

Intelligence Information. Information that is under the jurisdiction and control of the Director of Central Intelligence or a member of the Intelligence Community.

Intelligent Terminal. An AIS term that means a terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics.

Letter of Consent. The form used by the CSA to notify a contractor that a PCL or a Limited Access Authorization has been granted to an employee.

Letter of Offer and Acceptance (LOA). United States Department of Defense Offer and Acceptance that, when executed, provides that the U.S. offers to sell, subject to terms and conditions contained therein, defense material to a foreign government, and the foreign government accepts the offer, subject to those terms and conditions.

Military Export Sales. Military Export Sales may be divided into Foreign Military Sales (FMS) under the AECA, sales under Section 607 of the Foreign Assistance Act (FAA) and Direct Commercial Sales. FMS and FAA are government-to-government transactions. For these sales, the DoD purchases articles and services from U.S. firms, takes title to the equipment, or has title to the articles to be sold from U.S. stocks, and sells the articles or services to the foreign buyer. For direct commercial sales, the U.S. firm sells directly to the foreign government or international organization.

Limited Access Authorization. Security access authorization to CONFIDENTIAL or SECRET information granted to non-U. S. citizens requiring such limited access in the course of their regular duties.

Material. Any product or substance on, or in which, information is embodied.

Multiple Facility Organization. A legal entity (single proprietorship, partnership, association, trust, or corporation) that is composed of two or more facilities.

National of the United States. A national of the United States is: a. A citizen of the United States, or, b. A person who, though not a citizen of the United States, owes permanent allegiance to the United States.

NOTE: 8 U.S. C. 1101(a) (22), 8 U.S. C. 1401, subsection (a) lists in paragraphs (1) through (7) categories of persons born in and outside the United States or its possessions who may qualify as nationals of the United States. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a national of the United States.

National Security. The national defense and foreign relations of the United States.

National Security Information. Any information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is so designated. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information and it is referred to as “classified information.”

NATO Information. Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless proper NATO authority has been obtained to release outside of NATO.

Need-to-Know. A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

Network. An AIS term meaning a network composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required. (Only government officials, who have been designated in writing, may apply an original classification to information.)

Parent Corporation. A corporation that owns at least a majority of another corporation’s voting securities.

Personnel (Security) Clearance. An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Possessions. U.S. possessions are the U.S. Virgin Islands, Guam, American Samoa, Swain’s Island, Howland Island, Baker Island, Jarvis Island, Midway Islands (this consists of Sand Island and Eastern

Island), Kingman Reef, Johnston Atoll, Navassa Island, Swan Island, Wake Island, and Palmyra Island.

Prime Contract. A contract let by a GCA to a contractor for a legitimate government purpose,

Prime Contractor. The contractor who receives a prime contract from a GCA.

Proscribed Information.

- a. Top Secret information;
- b. Communications Security (COMSEC) information, except classified keys used to operate secure telephone units (STU 111s);
- c. Restricted Data as defined in the U.S. Atomic Energy Act of 1954, as amended;
- d. Special Access Program (SAP) information; or
- e. Sensitive Compartmented Information

Protective Security Service. A transportation protective service provided by a cleared commercial carrier qualified by the Military Traffic Management Command (MTMC) to transport SECRET shipments.

Public. Any contractor, subcontractor, Government official, or other individual who does not require access to information (classified or unclassified) in furtherance of the performance of the classified contract under which the information was provided to the contractor or as authorized by this Manual.

Public Disclosure. The passing of information and/or material pertaining to a classified contract to the public, or any member of the public, by any means of communication.

Reference Material. Documentary material over which the GCA, who lets the classified contract, does not have classification jurisdiction, and did not have classification jurisdiction at the time the material was originated. Most material made available to contractors by the Defense Technical Information Center and other secondary distribution agencies is reference material as thus defined.

Regrade. To assign a higher or lower security classification to an item of classified material.

Remote Terminal. A device for communication with an automated information system from a location, that is not within the central computer facility.

Representative of a Foreign Interest (RFI). A citizen or national of the United States, who is acting as a representative of a foreign interest. (See “Foreign Interest.”)

Restricted Area. A controlled access area established to safeguard classified material, that because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

Restricted Data. All data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.

SECRET. The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Security Cognizance. The Government office assigned the responsibility for acting for CSAS in the discharge of industrial security responsibilities described in this Manual.

Security in Depth. A determination made by the CSA that a contractor’s security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

Security Violation. Failure to comply with the policy and procedures established by this Manual that reasonably could result in the loss or compromise of classified information.

Sensitive Compartmented Information. All Intelligence Information and material that requires special controls for restricted handling within compartmented channels and for which compartmentation is established.

Shipper. One who releases custody of material to a carrier for transportation to a consignee. (See “Consignor.”)

Short Title. An identifying combination of letters and numbers assigned to a document or equipment for purposes of brevity.

Source Document. A classified document, other than a classification guide, from which information is extracted for inclusion in another document.

Special Access Program. Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 12958. I

Standard Practice Procedures. A document(s) prepared by a contractor that implements the applicable requirements of this Manual for the contractor’s operations and involvement with classified information at the contractor’s facility.

Subcontract. Any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract. For purposes of this Manual a subcontract is any contract, subcontract, purchase order, lease agreement, service agreement, request for quotation (RFQ), request for proposal (RFP), invitation for bid (IFB), or other agreement or procurement action between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract.

Subcontractor. A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor. For purposes of this Manual, each subcontractor shall be considered as a prime contractor in relation to its subcontractors.

Subsidiary Corporation. A corporation in which another corporation owns at least a majority of its voting securities.

System Software. Computer programs that control, monitor, or facilitate use of the AIS; for example, operating systems, programming languages,

communication, input-output control, sorts, security packages and other utility-type programs. Considered to also include off-the-shelf application packages obtained from manufacturers and commercial vendors, such as for word processing, spreadsheets, data base management, graphics, and computer-aided design.

Technical Data. Information governed by the International Traffic in Arms Regulation (ITAR) and the Export Administration Regulation (EAR). The export of technical data that is inherently military in character is controlled by the ITAR, 22 CFR 120.1-130.17 (1987). The export of technical data that has both military and civilian uses is controlled by the EAR, 15 CFR 368.1 -399.2 (1987).

TOP SECRET. The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Transclassification. When information has been removed from the RD category by a joint determination of DOE and DOD and placed in the FRD category in accordance with section 142d of the Atomic Energy Act.

Transmission. The sending of information from one place to another by radio, microwave, laser, or other nonconnective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

Transshipping Activity. A government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

United States and Its Territorial Areas. The 50 states, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Virgin Islands, the Trust Territory of the Pacific Islands (also called Micronesia), Midway Island, Wake Island, Johnston Atoll, Kingman Reef, Swain's Island, and Palmyra Island.

Unauthorized Person. A person not authorized to have access to specific classified information in accordance with the requirements of this Manual.

United States. The 50 states and the District of Columbia.

United States Citizen (Native Born). A person born in one of the following locations is considered to be a U.S. citizen for industrial security purposes: the 50 United States; District of Columbia; Puerto Rico; Guam; American Samoa; Northern Mariana Islands; U.S. Virgin Islands; Panama Canal Zone (if the father or mother (or both) was, or is, a citizen of the U.S.); the Federated States of Micronesia; and the Republic of the Marshall Islands.

U.S. Person. Any form of business enterprise or entity organized, chartered or incorporated under the laws of the United States or its possessions and trust territories and any person who is a citizen or national of the United States.

Upgrade. A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

Voting Securities. Any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

Working Hours. The period of time when:

a. There is present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled workshift; and

b. The number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.